UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/806,772	03/23/2004	Trevor W. Freeman	M1103.70185US01	2366

45840 7590 07/02/2007

WOLF GREENFIELD (Microsoft Corporation)
C/O WOLF, GREENFIELD & SACKS, P.C.
600 ATLANTIC AVENUE
BOSTON, MA 02210-2206

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/806,772	FREEMAN ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/23/07 & 5/23/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-2, 4, 6-9, 11, and 13-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Balissat, et al. (US 7,188,365).

As per claim 1:

Balissat discloses a method for establishing a secure communications channel and authenticating a party, for use by an initiator in an Internet Security Protocol (IPSec) negotiation **(col.1, lines 43-54 and col.9, lines 22-27)**, comprising:

initiating an Internet Key Exchange (IKE) negotiation with a responder; **(col.2, lines 40-43 and col.8, lines 4-6)**

transmitting, to the responder, a public Diffie-Hellman (DH) key of the initiator; **(col.2, lines 45-48; device 100 is the claimed initiator and that device 100 can also be a firewall or gateway 110 (col.7, lines 57-59), but may also be the a responder that exchange(s) with device 140 (col.10, lines 20-37). With either device being the initiator or responder, Balissat discloses both has a public DH key for exchange with each other (col.2, lines 45-48). By exchange keys to one another, Balissat suggests transmitting the initiator's public key to a responder and receiving from a responder the public key as claimed below. In addition, Balissat discloses in a Diffie-Hellman (DH) key exchange, two uses build a symmetric secret key (same key used for encryption and decryption) using their local private keys, a known DH key and the other device's public key (col.9, lines 27-33). Thus, this reads on the payload encrypted with a shared secret key claimed further below.)**

receiving, from the responder, a public DH key of the responder; **(col.9, lines 43-46; device 140 is referring to the claimed responder (col.8, lines 65-66) but may also be the one to initiate the exchange(s) and that the device 100 can be the responder (col.10, lines 20-32).)**

transmitting, to the responder, a payload encrypted **(col.7, lines 60-67)** with a shared secret created from the public DH key of the responder and the private DH key **(col.2, lines 48-52)** corresponding to the public DH key of the initiator transmitted to the responder; **(col.9, lines 38-48 and col.10, lines 10-14)**

receiving, from the responder, a payload encrypted with the shared secret; and **(col.10, lines 2-8 and col.11, lines 23-27)**

decrypting the payload; **(col.13, lines 53-55)**

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder **(col.3, lines 1-13)**, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator. **(col.12, lines 7-15 and col.13, lines 15-23)**

As per claim 2: See col.9, lines 38-67 and col.13, lines 15-23; discussing the method of claim 1 wherein the public DH key of the responder is previously known to the initiator and is a claim on the identity of the responder.

As per claim 4: See col.3, lines 1-13 and col.13, lines 15-23; discussing the method of claim 1 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

As per claim 6: See col.2, lines 13-15; discussing the method of claim 1 wherein the secure communications channel is a channel in a virtual private network (VPN).

As per claim 7: See col.2, lines 13-48; discussing the method of claim 6 wherein the VPN comprises a client and a server, and a public DH key of the VPN client is transmitted as a hint to the identity of the client.

As per claim 8:

Balissat discloses a method for establishing a secure communications channel and authenticating a party, for use by a responder in an Interact Security Protocol (IPSec) negotiation **(col.1, lines 43-54 and col.9, lines 22-27)**, comprising:

receiving an Internet Key Exchange (IKE) negotiation request from an initiator; **(col.2, lines 40-43 and col.8, lines 4-6)**

transmitting, to the initiator, a public Diffie-Hellman (DH) key of the responder; **(col.2, lines 45-48; device 100 is the claimed initiator and that device 100 can also be a firewall or gateway 110 (col.7, lines 57-59), but may also be the a responder that exchange(s) with device 140 (col.10, lines 20-37). With either device being the initiator or responder, Balissat discloses both has a public DH key for exchange with each other (col.2, lines 45-48). By exchange keys to one another, Balissat suggests transmitting the initiator's public key to a responder and receiving from a responder the public key as claimed below. In addition, Balissat discloses in a Diffie-Hellman (DH) key exchange, two uses build a symmetric secret key (same key used for encryption and decryption) using their local private keys, a known DH key and the other device's public key (col.9, lines 27-33). Thus, this reads on the payload encrypted with a shared secret key claimed further below.)**

receiving, from the initiator, a public DH key of the initiator; **(col.9, lines 43-46; device 140 is referring to the claimed responder (col.8, lines 65-66) but**

may also be the one to initiate the exchange(s) and that the device 100 can be the responder (col.10, lines 20-32).)

transmitting, to the initiator, a payload encrypted **(col.7, lines 60-67)** with a shared secret created from the public DH key of the initiator and the private DH key **(col.2, lines 48-52)** corresponding to the public DH key of the responder transmitted to the initiator; **(col.9, lines 38-48 and col.10, lines 10-14)**

receiving, from the initiator, a payload encrypted with the shared secret; and**(col.10, lines 2-8 and col.11, lines 23-27)**

decrypting the payload; **(col.13, lines 53-55)**

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder **(col.3, lines 1-13)**, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator. **(col.12, lines 7-15 and col.13, lines 15-23)**

As per claim 9: See col.3, lines 1-13 and col.9, lines 38-67; discussing the method of claim 8 wherein the public DH key of the responder is previously known to the initiator and is a claim on the identity of the responder.

As per claim 11: See col.13, lines 15-23 and col.13, lines 15-23; discussing the method of claim 8 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

As per claim 13: See col.2, lines 13-15; discussing the method of claim 8 wherein the secure communications channel is a channel in a virtual private network (VPN).

As per claim 14: See col.2, lines 13-48 and col.13, lines 15-23; discussing the method of claim-13 wherein VPN comprises a client and a server, and a public DH key of the VPN client is received as a hint to the identity of the client.

As per claim 15:

Balissat discloses a method of establishing, between an initiator and a responder **(col.8, lines 65-67 and col.10, lines 20-32)**, a secure communications channel following the Internet Security Protocol (IPSec) **(col.1, lines 43-54 and col.9, lines 22-27)**, comprising using the Internet Key Exchange (IKE) protocol **(col.2, lines 40-43 and col.3, lines 1-13)**, wherein a static Diffie-Hellman (DH) key-pair **(col.8, lines 4-6 and col.9, lines 25-46)** is used by at least one of the initiator or the responder to establish confidentiality and authentication. **(col.7, lines 60-67 and col.13, lines 15-23)**

As per claim 16: See col.3, lines 1-13 and col.13, lines 15-23; discussing the method of claim 15 wherein the private DH key of the DH key-pair is used to create a claim of identity for the initiator or the responder.

As per claim 17: See col.2, lines 13-16; discussing the method of claim 15 wherein the secure communications channel is a channel in a virtual private network.

As per claim 20:

Balissat discloses a computer-readable medium including computer-executable instructions facilitating establishing a secure communications channel and authenticating a party, for execution by an initiator in an Internet Security Protocol (IPSec) negotiation **(col.1, lines 43-54 and col.9, lines 22-27)**, said computer-executable instructions executing the steps of:

initiating an Internet Key Exchange (IKE) negotiation with a responder; **(col.2, lines 40-43 and col.8, lines 4-6)**

transmitting, to the responder, a public Diffie-Hellman (DH) key of the initiator; **(col.2, lines 45-48; device 100 is the claimed initiator and that device 100 can also be a firewall or gateway 110 (col.7, lines 57-59), but may also be the a responder that exchange(s) with device 140 (col.10, lines 20-37). With either device being the initiator or responder, Balissat discloses both has a public DH key for exchange with each other (col.2, lines 45-48). By exchange keys to one another, Balissat suggests transmitting the initiator's public key to a responder and receiving from a responder the public key as claimed below. In addition, Balissat discloses in a Diffie-Hellman (DH) key exchange, two uses build a symmetric secret key (same key used for encryption and decryption) using their local private keys, a known DH key and the other device's public key (col.9, lines 27-33). Thus, this reads on the payload encrypted with a shared secret key claimed further below.)**

receiving, from the responder, a public DH key of the responder; **(col.9, lines 43-46; device 140 is referring to the claimed responder (col.8, lines 65-66) but may also be the one to initiate the exchange(s) and that the device 100 can be the responder (col.10, lines 20-32).)**

transmitting, to the responder, a payload encrypted **(col.7, lines 60-67)** with a shared secret created from the public DH key of the responder and the private DH key

(col.2, lines 48-52) corresponding to the public DH key of the initiator transmitted to the responder; **(col.9, lines 38-48 and col.10, lines 10-14)**

receiving, from the responder, a payload encrypted with the shared secret; and**(col.10, lines 2-8 and col.11, lines 23-27)**

decrypting the payload; **(col.13, lines 53-55)**

wherein the public DH key of the responder is a claim on the identity of the responder and the shared secret is used to authenticate the identity of the responder **(col.3, lines 1-13)**, or the public DH key of the initiator is a claim on the identity of the initiator and the shared secret is used to authenticate the identity of the initiator. **(col.12, lines 7-15 and col.13, lines 15-23)**

As per claim 21: See col.9, lines 38-67 and col.13, lines 15-23; discussing the computer-readable medium of claim 20 wherein the public DH key of the responder is previously known to the initiator and is as a claim on the identity of the responder.

As per claim 22: See col.3, lines 1-13 and col.13, lines 15-23; discussing the computer-readable medium of claim 20 wherein the public DH key of the initiator is previously known to the responder and is a claim on the identity of the initiator.

As per claim 23: See col.2, lines 13-16; discussing the computer-readable medium of claim 20 wherein the secure communications channel is a channel in a virtual private network.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 3, 5, 10, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Balissat, et al. (US 7,188,365), and further in view of Daly, et al. (US 5,930,362).

As per claim 3: Balissat discloses the method of claim 4 wherein a responder has previously obtained the public DH key of the initiator (col.9, lines 27-48) but fails to include from a portable media device.

Daly discloses a method for creating a plurality of Diffie-Hellman data encryption values for subsequent transmission where these shared secret data values are stored on the mobile station and the cellular network (col.1, lines 13-15 and 52-61). Daly discusses the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses (col.1, lines 22-25). A mobile station obviously allows mobility and accessible anywhere rather than at a fixed computing device where this limits a user to a certain location.

Therefore it would have been obvious for a person of ordinary skills in the art to combine Balissat with Daly teaching obtaining key information from a portable media

device because the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses with limiting to a fixed location (Daly – col.1, lines 22-25).

As per claim 5: Balissat discloses the method of claim 4 wherein the initiator has previously obtained the public DH key of the responder (col.9, lines 27-48 and col.10, lines 5-14) but fails to include from a portable media device.

Daly discloses a method for creating a plurality of Diffie-Hellman data encryption values for subsequent transmission where these shared secret data values are stored on the mobile station and the cellular network (col.1, lines 13-15 and 52-61). Daly discusses the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses (col.1, lines 22-25). A mobile station obviously allows mobility and accessible anywhere rather than at a fixed computing device where this limits a user to a certain location.

Therefore it would have been obvious for a person of ordinary skills in the art to combine Balissat with Daly teaching obtaining key information from a portable media device because the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses with limiting to a fixed location (Daly – col.1, lines 22-25).

As per claim 10: Balissat discloses the method of claim 9 wherein the responder has previously obtained the public DH key of the initiator (col.9, lines 27-48) but fails to include from a portable media device.

Daly discloses a method for creating a plurality of Diffie-Hellman data encryption values for subsequent transmission where these shared secret data values are stored on the mobile station and the cellular network (col.1, lines 13-15 and 52-61). Daly discusses the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses (col.1, lines 22-25). A mobile station obviously allows mobility and accessible anywhere rather than at a fixed computing device where this limits a user to a certain location.

Therefore it would have been obvious for a person of ordinary skills in the art to combine Balissat with Daly teaching obtaining key information from a portable media device because the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses with limiting to a fixed location (Daly – col.1, lines 22-25).

As per claim 12: Balissat discloses the method of claim 11 wherein the initiator has previously obtained the public DH key of the responder (col.9, lines 27-48 and col.10, lines 5-14) but fails to include from a portable media device.

Daly discloses a method for creating a plurality of Diffie-Hellman data encryption values for subsequent transmission where these shared secret data values are stored

on the mobile station and the cellular network (col.1, lines 13-15 and 52-61). Daly discusses the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses (col.1, lines 22-25). A mobile station obviously allows mobility and accessible anywhere rather than at a fixed computing device where this limits a user to a certain location.

Therefore it would have been obvious for a person of ordinary skills in the art to combine Balissat with Daly teaching obtaining key information from a portable media device because the presence of shared secret data on a mobile station and a cellular network allows sophisticated bi-directional verification techniques to be implemented for authentication of the mobile station to the cellular network in subsequent uses with limiting to a fixed location (Daly – col.1, lines 22-25).

4. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daly, et al. (US 5,930,362), and further in view of Balissat, et al. (US 7,188,365).

As per claim 18:

Daly discloses a system for establishing a secure communications channel between networked devices comprising: a first networked device generating a Diffie-Hellman (DH) key pair **(col.1, lines 59-61 and col.3, lines 30-33)**; a portable media

device storing the DH key pair generated by the first networked device **(col.1, lines 13-15 and col.4, lines 47-50)**; and a second networked device reading the DH key pair from the portable media device **(col.2, lines 32-363, lines 16-20)**; the second networked device using the DH key pair to ensure confidentiality and authenticity in securing a communications channel with another networked device **(col.1, lines 22-25 and col.3, lines 34-48)**, [*following the Internet Key Exchange (IKE) and Internet Security (IPSec) protocols]*.

However, Daly did not include Internet Key Exchange (IKE) and Internet Security (IPSec) protocols.

Balissat discloses a method for implementing secure network communications between a first device and a second device (col.4, lines 22-25) that initiates a session for the first of the two conventional phases in negotiating an SA using IKE (col.8, lines 4-6). The SA operations applied to packets include an authentication method, encryption method, and authentication/encryption keys where IKE allows two devices to negotiate and agree on these operations including establishment of the keys (col.7, lines 60-67). Balissat further explains the IKE typically operates in two phases, a first phase is where parties agree as to how to protect further negotiation traffic (i.e. IKE may authenticate a sender by Diffie-Hellman encryption) and the second phase is where IKE negotiates the actual IPsec SA by setting up the encryption/authentication keys for the AH and/or ESP protocols (col.2, lines 40-52 and col.3, lines 10-12). Balissat discusses a particular conventional protocol for providing security between devices operating over

an Internet Protocol (IP) network is known as IPsec. IPsec is a set of protocols supporting the secure exchange of IP packets at a network layer (col.1, lines 48-52).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Daly with Balissat to teach Internet Key Exchange (IKE) and Internet Security (IPSec) protocols because IKE parties agree as to how to protect further negotiation traffic negotiates and the actual IPsec SA by setting up the encryption/authentication keys for the AH and/or ESP protocols (Balissat – col.2, lines 40-52 and col.3, lines 10-12) and IPsec protocol is a conventional protocol for providing security between devices operating over an Internet Protocol (IP) network that supports the secure exchange of IP packets at a network layer (Balissat – col.1, lines 48-52).

As per claim 19: See Balissat on col.2, lines 13-16; discussing the system of claim 18 wherein the secure communications channel is a channel in a virtual private network.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax

phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

HOSUK SONG
PRIMARY EXAMINER